

# Sémantique de test quantitative

## Calculs de processus algébriques, épisode 2

Emmanuel Beffara



Institut de Mathématiques de Luminy  
CNRS & Université Aix-Marseille II



**choco**

Lyon, 18 juin 2009

On cherche un cadre sémantique pour la concurrence :

- ▶ qui soit dénotationnel,
- ▶ qui tienne compte du non-déterminisme,
- ▶ qui ait de bonnes propriétés algébriques.

Pourquoi des combinaisons linéaires ?

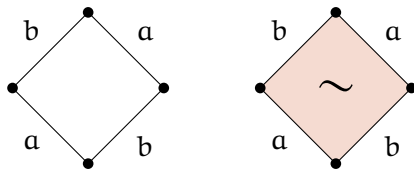
- ▶ faire grossir l'espace pour gagner en généralité,
- ▶ donner de la place pour étendre le calcul (probas, quantique),
- ▶ renforcer le lien avec les réseaux,
- ▶ utiliser des maths existantes.

L'introduction d'une somme formelle idempotente faisait apparaître :

- ▶ une notion d'incohérence :  $0$
- ▶ des actions linéaires :  $\hat{a}.P$
- ▶ décomposition des actions affines :  $a.P = \hat{a}.P \oplus a.0$
- ▶ décomposition du choix :  $a.P \& b.Q = \hat{a}.P \oplus \hat{b}.Q \oplus a.0 \mid b.0$
- ▶ la loi de développement :  $\hat{a}.P \mid \hat{b}.Q = \hat{a}.(P \mid \hat{b}.Q) \oplus \hat{b}.(a.P \mid Q)$

# Entrelacement

Le cas standard :



$$a.b + b.a \neq a | b$$

Qu'est-ce qui différencie « observationnellement » ces deux processus ?

Le nombre de chemins !

- ▶ On part d'un calcul de processus arbitraire **sans récursion** :

$P, Q := \alpha.P$	préfixe d'action
$P \mid Q$	composition parallèle
$(\nu \alpha)P$	restriction
$1$	inaction

- ▶ On part d'un calcul de processus arbitraire **sans récursion** :

$P, Q := \alpha.P$	préfixe d'action
$P \mid Q$	composition parallèle
$(\nu \alpha)P$	restriction
$\lambda$	résultat

- ▶ On ajoute des résultats dans un semi-anneau  $\mathbb{K}$

$\lambda + \mu$	choix non déterministe	0	annulation
$\lambda \cdot \mu$	composition parallèle de résultats	1	neutralité

- ▶ Résultat de l'exécution d'un terme  $P$  :

$\langle P \rangle =$  somme des résultats finaux de toutes les exécutions  
**issues de choix différents.**

- ▶  $P = Q$  si pour tout  $R$ ,  $\langle P \mid R \rangle = \langle Q \mid R \rangle$ .

# (Comment définir la sémantique opérationnelle)

**termes**  $P, Q ::= a.P \quad P | Q \quad (\nu a)P \quad \lambda \dots$

**transitions**  $a.P \xrightarrow{a} P \quad \frac{P \xrightarrow{a} P' \quad Q \xrightarrow{\bar{a}} Q'}{P | Q \xrightarrow{\tau} P' | Q'} \dots$

# (Comment définir la sémantique opérationnelle)

**termes**  $P, Q ::= a_i.P \quad P | Q \quad (\nu a)P \quad \lambda \quad \dots$

**localités**  $i, j$  dans un ensemble partiellement ordonné,  
par exemple les positions dans le terme de départ

**transitions**  $a_i.P \xrightarrow{a:i} P$        $\frac{P \xrightarrow{a:i} P' \quad Q \xrightarrow{\bar{a}:j} Q'}{P | Q \xrightarrow{\tau:i,j} P' | Q'} \quad \dots$

# (Comment définir la sémantique opérationnelle)

**termes**  $P, Q ::= a_i.P \quad P \mid Q \quad (\nu a)P \quad \lambda \quad \dots$

**localités**  $i, j$  dans un ensemble partiellement ordonné,  
par exemple les positions dans le terme de départ

**transitions**  $a_i.P \xrightarrow{a:i} P \quad \frac{P \xrightarrow{a:i} P' \quad Q \xrightarrow{\bar{a}:j} Q'}{P \mid Q \xrightarrow{\tau:i,j} P' \mid Q'} \quad \dots$

**homotopie**  $P \xrightarrow{a:i} Q \xrightarrow{b:j} R \sim P \xrightarrow{b:j} Q' \xrightarrow{a:i} R \quad \text{si } i \parallel j$

**pré-traces** multi-ensembles d'étiquettes partiellement ordonné  
(en fonction de l'ordre sur les localités)

**exécutions** pré-traces maximales composées de  $\tau$

# (Comment définir la sémantique opérationnelle)

**termes**  $P, Q ::= a_i.P \quad P \mid Q \quad (\nu a)P \quad \lambda \quad \dots$

**localités**  $i, j$  dans un ensemble partiellement ordonné,  
par exemple les positions dans le terme de départ

**transitions**  $a_i.P \xrightarrow{a:i} P \quad \frac{P \xrightarrow{a:i} P' \quad Q \xrightarrow{\bar{a}:j} Q'}{P \mid Q \xrightarrow{\tau:i,j} P' \mid Q'} \quad \dots$

**homotopie**  $P \xrightarrow{a:i} Q \xrightarrow{b:j} R \sim P \xrightarrow{b:j} Q' \xrightarrow{a:i} R \quad \text{si } i \parallel j$

**pré-traces** multi-ensembles d'étiquettes partiellement ordonné  
(en fonction de l'ordre sur les localités)

**exécutions** pré-traces maximales composées de  $\tau$

Ou alors, configurations maximales dans des structures d'événements.

- ▶ Congruence pour toutes les opérations du calcul.
- ▶ Lois de  $\mathbb{K}$ -module avec les opérations suivantes :

$$P \oplus Q := (\nu a)(a.P \mid a.Q \mid \bar{a}.1)$$
$$\lambda \cdot P := \lambda \mid P$$

- ▶ Linéarité des opérations du calcul, sauf l'action :

$$\alpha.P = \hat{\alpha}.P \oplus \alpha.0 \quad \text{affine}$$

où

$$\hat{\alpha}.P := (\nu w)(\alpha.w.P \mid w.0 \mid \bar{w}.1) \quad \text{linéaire}$$

- ▶ La fonction « résultat »  $\langle P \rangle$  est une forme linéaire.

On a donc la définition d'un espace des processus finis.

Le programme de la suite :

1. déconstruction de l'espace,  
pour en trouver une base ;
2. reconstruction des opérations du calcul,  
étendues aux processus récursifs.

Par linéarité, on décompose tous les termes en combinaisons linéaires de termes simples :

$S, T := \hat{a}.S$	action linéaire
$a.0$	inaction
$S   T$	composition parallèle
$1$	neutre
$(\nu a)S$	restriction

Les résultats sont dans  $\mathbb{N}$ .

- ▶ Syntactiquement, une pré-trace :

$$P_0 \xrightarrow{a:i} P_1 \xrightarrow{\tau:j,k} P_2 \xrightarrow{b:l} P_3 \dots$$

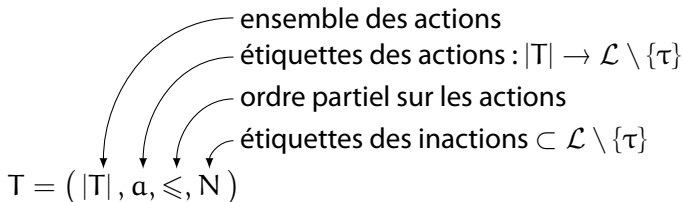
à commutation près des actions indépendantes

- ▶ Syntactiquement, une trace :

$$P_0 \xrightarrow{a:i} P_1 \xrightarrow{\tau:j,k} P_2 \xrightarrow{b:l} P_3 \dots$$

à commutation près des actions indépendantes

- ▶ Plus abstraitement, pour CCS :



- ▶ Syntactiquement, une trace :

$$P_0 \xrightarrow{a:i} P_1 \xrightarrow{\tau:j,k} P_2 \xrightarrow{b:l} P_3 \dots$$

à commutation près des actions indépendantes

- ▶ Plus abstraitement, pour CCS :

$$T = (|T|, \alpha, \leq, N)$$

ensemble des actions  
étiquettes des actions :  $|T| \rightarrow \mathcal{L} \setminus \{\tau\}$   
ordre partiel sur les actions  
étiquettes des inactions  $\subset \mathcal{L} \setminus \{\tau\}$

- ▶ On peut implémenter les traces

moyennant une composition parallèle sans interaction,

un terme simple est la somme de ses traces.

Synchronisation de deux traces  $T$  et  $U$  :

- ▶ une bijection  $\sigma : |T| \rightarrow |U|$ ,
- ▶ pour tout  $x \in |T|$ ,  $\alpha(x) = \overline{\alpha(\sigma(x))}$ ,
- ▶ les ordres  $\leq_T$  et  $\leq_U$  sont compatibles,
- ▶ pour tout  $x \in N_T$ ,  $\bar{x} \notin N_U$ .

Résultat de l'interaction :

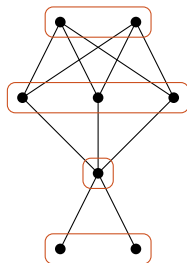
$$\langle T \mid U \rangle = \text{nombre de synchronisations}$$

Les autres opérations se définissent facilement.

# Une base de l'espace des processus finis

Deux cas :

- ▶ Si dans  $\mathbb{K}$ ,  $\forall x, x + x = x$ ,  
alors les traces totalement ordonnées forment une base.
- ▶ Si  $\mathbb{K}$  est un anneau qui étend  $\mathbb{Z}$ ,  
alors les traces *étagées* forment une base.



- ▶ Produit tensoriel des traces simples et des inactions.

# Les comportements infinis

Soit  $\mathcal{T}$  le  $\mathbb{K}$ -module des processus finis (les tests).

**comportement** = forme linéaire sur  $\mathcal{T}$

Pour  $P \in \mathcal{T}$ ,  $P^* : Q \mapsto \langle P \mid Q \rangle$ .

**comportement partiel** = forme linéaire sur un sous-module

Il y a plus de comportements que de tests.

# Opérations syntaxiques simples

Si  $f$  est le comportement d'un terme  $P$ ,

- ▶ composition avec un terme fini

$$\langle (P \mid Q) \mid R \rangle = \langle P \mid (Q \mid R) \rangle \quad (f \mid Q)(R) := f(Q \mid R)$$

- ▶ restriction

$$\langle (\nu a)P \mid Q \rangle = \langle P \mid (\nu a)Q \rangle \quad ((\nu a)f)(Q) := f((\nu a)Q)$$

- ▶ action linéaire

$$\langle \hat{a}.P \mid Q \rangle = \left\langle P \mid \frac{\partial Q}{\partial a} \right\rangle \quad (\hat{a}.f)(Q) := f\left(\frac{\partial Q}{\partial a}\right)$$

où  $\partial Q / \partial a$  est la somme des  $Q'$  tels que  $Q \xrightarrow{\bar{a}} Q'$   
(à peu de chose près).

# Exemple

Soit l'équation  $\mathbf{X} = \mathbf{a} \cdot (\mathbf{P} \mid \mathbf{X})$  avec  $\mathbf{a} \notin \text{fn}(\mathbf{P})$ .

Une solution  $f$  doit vérifier  $f(Q) = \langle \mathbf{a} \cdot 0 \mid Q \rangle + f\left(\mathbf{P} \mid \frac{\partial Q}{\partial \mathbf{a}}\right)$ ,

d'où  $f(Q) = \sum_{i=0}^n \langle \mathbf{a} \cdot 0 \mid Q_i \rangle + f(Q_{n+1})$  avec  $Q_n = \frac{\partial^n(\mathbf{P}^n \mid Q)}{\partial \mathbf{a}^n}$

or  $Q_n = 0$  à partir d'un certain rang donc

$$f(Q) = \sum_{n=0}^{\infty} \left\langle \mathbf{a} \cdot 0 \mid \frac{\partial^n(\mathbf{P}^n \mid Q)}{\partial \mathbf{a}^n} \right\rangle \quad f = \lim_{n \rightarrow \infty} \underbrace{\left( \mathbf{a} \cdot (\mathbf{P} \mid \mathbf{a} \cdot (\mathbf{P} \mid \dots \mid \mathbf{a} \cdot \mathbf{P})) \right)}_{n \text{ fois } \mathbf{a}}^*$$

# Questions topologiques

Soient les suites de termes

$$P_n = \underbrace{a.a \dots a}_n$$

$$Q_n = \underbrace{\bar{a}.\bar{a} \dots \bar{a}}_n$$

- ▶ Les suites  $(P_n^*)$  et  $(Q_n^*)$  convergent point par point (vers  $!a$  et  $!\bar{a}$ );
- ▶ Pour tout test  $R$  sans action sur  $a$ ,  $\langle P_i \mid Q_j \mid R \rangle = \langle R \rangle$ ;
- ▶ Si  $R$  contient au moins une action sur  $a$ ,  $\langle P_i \mid Q_j \mid R \rangle$  diverge.

# Questions topologiques

Soient les suites de termes

$$P_n = \underbrace{a.a \dots a}_n$$

$$Q_n = \underbrace{\bar{a}.\bar{a} \dots \bar{a}}_n$$

- ▶ Les suites  $(P_n^*)$  et  $(Q_n^*)$  convergent point par point (vers  $!a$  et  $!\bar{a}$ );
- ▶ Pour tout test  $R$  sans action sur  $a$ ,  $\langle P_i \mid Q_j \mid R \rangle = \langle R \rangle$ ;
- ▶ Si  $R$  contient au moins une action sur  $a$ ,  $\langle P_i \mid Q_j \mid R \rangle$  diverge.

Un autre exemple :

$$\begin{aligned}(\nu a)(\bar{a} \mid !a.\bar{a} \mid a.b) &= \text{divergence} \\(\nu a)(\bar{a} \mid !a.(\frac{1}{2} \mid \bar{a}) \mid a.b) &= 2 \cdot b\end{aligned}$$

Enjeu : trouver les bonnes topologies pour différentes formes de test.

Questions ?